



TRANSPARENCY REPORT

April 2022 – September 2022

Index

1. [Introduction](#)
2. [Policy and Legal Composition](#)
3. [Investor Protection](#)
4. [Law Enforcement Request](#)
5. [Fraud Detection and Prevention](#)
6. [Building on our Transaction Monitoring Foundation](#)
7. [WazirX Monitoring Approach](#)
8. [Policy Outreach](#)
9. [Collaborations](#)

Introduction

Keeping up with its record of maintaining transparency, coordinating with law enforcement establishments, and providing a secure trading ecosystem for investors in the country, WazirX brings you the third version of the Transparency Report.

This report covers an overview of initiatives that the company took during the months of April to September '22 to safeguard users in the virtual digital asset (VDA) ecosystem. It also includes details on requests for user data, content, and account restrictions by Indian and Foreign law enforcement agencies.

During the above-mentioned time period, 828 requests were received from Law Enforcement agencies (LEA), against a total of 10Mn transactions on the platform during this period. 64 requests were from Foreign LEAs and 764 requests from Indian LEAs.

All of these requests pertained to matters where criminal proceedings, investigation, and inquiry were initiated against the accused persons, and information was sought from WazirX as to whether such accused had dealt in Crypto through our platform. WazirX promptly provided all information as sought, and our compliance rate in record timeliness and accuracy was 100%. Apart from that, blocking of over 700 accounts was also initiated based on our internal transaction monitoring process and/or directives from the LEAs.

In recent times, we marked the initiation of the #BuildforBharat Campaign. The educational series covered ten potential industries in India and how blockchain technology and Crypto can influence them. WazirX also joined hands with other industry players in the country to form a new crypto advocacy group called Bharat Web3 Association (BWA). This group will enable the members to stay in touch with regulators in the industry, apprise them of developments within the ecosystem, and also protect consumer interests.

WazirX proactively reported suspicious transactions to law enforcement agencies such as the Financial Intelligence Unit, India (FIU-IND). The team reported transactions of suspicious nature, wherein the trading volumes of users were not aligned with individual ITR/financial status/income, transactions by users were deemed to be high-risk ones as per alerts

received from third-party forensic tools, and also such users who did not provide the information/clarifications sought as regards to the source of funds or income proof.

Policy and Legal Composition

At WazirX, we are diligent in protecting our stakeholders' personal information, transactional data, and financial data. We also maintain absolute transparency while catering to information requests from government and law enforcement agencies.

- We have a well-equipped policy and legal team to review, coordinate and comply with concerned authorities.
- Internal systems, processes, and procedures are carefully reviewed and modified based on previous requests from various agencies and the observations found therein.
- Our user agreements/terms and conditions duly bind the user to provide any information as may be sought by us in connection with their account/transactions and share any information/details of their account/transactions with LEAs if demanded.

Partnership with Intelligence firms

WazirX's ongoing collaboration with third-party forensic tool service providers such as TRM Labs and Chainalysis has led to effective internal transaction monitoring and investigation, wallet screening, and risk management. The partnership has sustained the compliance initiatives of the platform and has helped us to not only give a speedier response to LEAs on their information requests but also assist them by participating in their investigation process.

Investor Protection

KYC Authentication

- WazirX is committed to ensuring that the most stringent KYC norms are followed for onboarding customers on its platform.

- To ensure that only legitimate users access our platform, access is allocated only to verified users who are identifiable with KYC documents. Processes are in place to allow money transfers from the user-owned whitelisted & linked bank account. The bank whitelisting works as a secondary KYC verification as well.
- We routinely do a hygiene check to block all bad actors from our platform based on KYC deficiencies or irregularities found during normal scrutiny/reverification.
- Product upgrades are regularly floated throughout the year.
- We monitor for fraud/document deficiency/tampering of records, and discourage customers on our platform who are suspected to be associated with these activities.
- One customer can have only one account with us (using a particular KYC credential such as PAN, Aadhaar etc) and the system would not permit an already registered user to once again open an account.

KYC Verification

On WazirX, for KYC verification, the PAN Card is mandatory. Along with this, every user has to submit any one of these: Aadhaar/Passport/Driving Licence. No user is onboarded without this verification. WazirX's KYC terms and processes are available on the platform publicly for prospective users to refer to. Because of this, for every transaction, WazirX is able to produce the KYC details of the relevant user.

Bank Verification

Bank verification works as the second layer check to ensure that the user is a genuine entity. We use the 'Penny Drop' technique wherein a token amount (Rs. 1) is deposited in the User's bank account proposed to be registered with us, and depending on the output file of the bank, it is checked if the name credentials match with the respective user. The existence of the account is thus verified and the account details are matched with the account holder's name as per their PAN and Aadhaar/Passport/Driving Licence. Bank transfers are only available for whitelisted accounts.

2 Factor Authentication (2FA) and Login

To ensure there is safety and no misuse, we have given our users 2 options for setting up a 2 factor authentication process:

- 2FA via SMS OTP
- 2FA via Authenticator app - Google Authenticator, Authy (More Secure)

Our support team identifies accounts which should be blocked based on suspicious trading activity. Thereby users are blocked from the system.

Flow of Transaction for a Centralized Crypto Exchange

Step 1 - User registers on the exchange using an email ID.

Step 2 - User submits KYC documents: PAN card and address proof (Compulsory Step - User cannot go forward without this).

Step 3 - The system at the back end checks national database through third-party verification agencies.

Step 4 - Photo is captured from the app and is matched against the KYC documents. A live photo (live selfie) is taken to ascertain against fake photos being submitted and also to ensure that a living/existing person is opening the account.

Step 5 - Bank verification happens after the user enters the Bank and/or UPI ID. The check is done by the penny drop testing and also, details are matched against the PAN Data submitted in the above steps. Here, API calls happen between WazirX and payment partners who facilitate the penny drop service post, which the Bank/UPI is marked verified.

Step 6 - Only after these steps are done can the user transfer the money to transact on the platform either through a bank account or an aggregator's account. A verification is again done to check the prima facie legitimacy of the source account and whether it is in India or not.

Step 7 - At this stage, a very small percentage of users also directly bring their VDAs to trade on the platform. They might have had VDAs through airdrops or mining or from trading on another platform.

Step 8 - With respect to P2P trades, users can purchase USDT with INR. With the USDT in their account, they can buy ETH, BTC, or any other VDA. The buyer's order is matched with the seller's order placed in the order book. The buyer receives the required VDA and the seller receives the USDT after the trade execution. This is done via the exchange open order book concept.

Step 9 - The user can HODL the crypto or can sell it and withdraw the money out to his/her linked bank account in the form of INR.

Customer Support

- To enhance user experience, address user queries, and increase touchpoints, we have created multiple channels. These include chatbots and in-house customer support teams. We upscaled our teams and technology as there is a need for user support at different stages - from account setup to individual trades and beyond.
- For assistance, we have dedicated support teams across chat, email, and social media who have engaged in over 700,000 user interactions which has resulted in high customer satisfaction scores even in this quarter.

User Support

WazirX also verifies user details with the National Securities Depository Limited (NSDL) (government) database based on the PAN. We also check the authenticity of the ID uploaded as address proof through third-party verification agencies.

Post KYC verification, users can transact and trade VDAs on the platform. We have a sophisticated process to ensure that only verified investors and traders use the WazirX platform. There could be one or more reasons that KYC verification may not be approved, and users can appeal through our 24X7 Support page - <https://support.wazirx.com/>

The most common reasons for rejection noticed are:

- **Details Mismatch** - When user's details like name, address, and ID Card number do not match the KYC documents submitted, KYC is rejected.
Here, as a point of note for users, we suggest cross-checking all details before submitting.
- **Duplicate Account** - KYC is rejected when a user attempts to create an account on WazirX with previously submitted or identical details (of another WazirX account). A user can have only one individual account. However, he/she can be an authorized signatory in other accounts in the case of corporates.

WazirX Support during April to September 2022

As mentioned above, we have upscaled our teams and technology to assist our users. Because of this, we have:

- Increased ticket handling adeptness.

- Enabled bots to handle straightforward deposit tickets (i.e., in an automated fashion), to increase efficiency.
- Enhanced our chat support wing.

Support Hours

To resolve account management queries (2FA reset, mobile number change, email ID change, etc.), P2P transfers, VDA deposit/withdrawals related, and other queries, our teams are available between 8 AM to 2 AM, Monday to Friday.



Law Enforcement Requests

Nature of Requests

All requests received from Indian as well as Foreign Enforcement Agencies were related to investigations wherein criminal proceedings were initiated against the accused.

Suspension/Blocking of Users Accounts

Suspension/Blocking of a user's account is subject to our terms and conditions i.e., when there is a violation of policies, deficient or suspicious KYC, or if we notice our platform is being used for illegal activities, we suspend/block the account of the user. We also have systems to monitor abnormal transactions done by users, flag off their related accounts, and identify other suspicious behavior so that these transactions can be reported to LEA if deemed fit.

Our compliance rate has been 100% for providing information/records to LEAs and also for abiding by their directives.

Turnaround Time

The recommended statutory Turnaround Time (TAT) for responding to the Law Enforcement Agencies (LEA) requests is up to 72 hrs from the time a request is received. However, with the help of efficient communication channels, WazirX clocked an average TAT as miniscule as 18 minutes for sending the first cut reply.

Here, by augmenting digital monitoring capabilities and with on-point communication channels with LEAs, we could help track fraudulent activities, which eventually resulted in the successful closure of requests.

Process for Raising a Law Enforcement Request

To submit a Law Enforcement request under relevant provisions of law, the requester must be a law enforcement agent or government official authorized to:

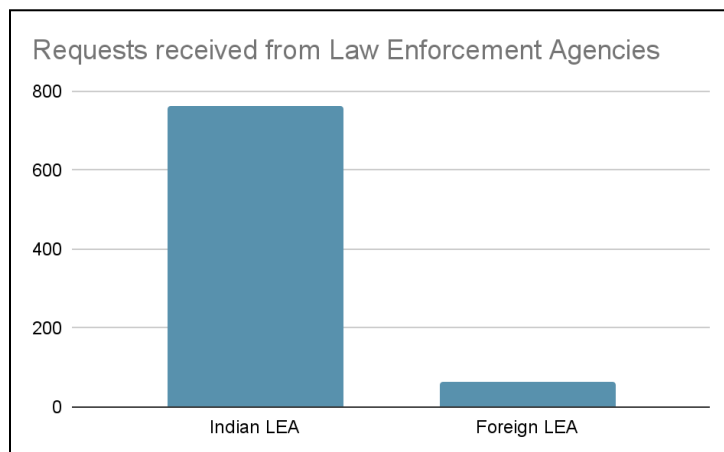
- Gather evidence in connection with an investigation, or
- Make a formal law enforcement request.


The following set-up is provided to law enforcement agents or government officials looking to obtain information from WazirX, in accordance with law, to gather evidence in connection with an ongoing legal proceeding.

Procedure:

- **Email request:** The requester can send an email to legal@wazirx.com from the official email ID of the law enforcement agency along with a duly authorized written request.
- **Scrutiny:** This email is scrutinized along with the details of the complaint, investigating officer, and seal of the agency.
- **Action:** If convinced with the scrutiny, appropriate action, as requested, is initiated from our end.

Some of the Indian and Foreign Law Enforcement Agencies that WazirX has worked with during this period are: the National Investigation Agency, Enforcement Directorate, State Cyber Crime Cells, Intelligence Fusion & Strategic Ops (IFSO) Delhi, Special Task Force, Narcotics Control Bureau, Bhopal Police, Crime Branch and CID, Toronto Police Department, Federal Bureau of Investigation (FBI), German Police Agencies, United Kingdom Police, Interpol, Dutch Police, Austrian Police, Europol, etc.



A red octagonal icon with the word 'STOP' in white, followed by the word 'FRAUD' in white on a red rectangular background.

Fraud Detection and Prevention

With our regular coordination with LEAs and further analysis of the received requests, we can detect many nefarious activities in the VDA space:

Impersonation Scams: With the rise in social media, imposters are successfully leveraging the technology and improving their reach to connect with VDA users. This is done by assuming the identity of a famous and credible individual from the VDA industry. As a result, the victim is lured into transferring the demanded amount to the imposter's account.

In a recent case, a Bitcoin racket being run from Delhi came to the notice of the CBI on being alerted by the Austrian police. Imposters posed as Europol officers and other law enforcement agencies to tell their victims that their identities had been stolen and used for narcotics businesses. The criminals would target foreign nationals for the same. WazirX's legal team, with assistance from Chainalysis, collaborated with the CBI on this case to block the operation. They identified the accounts which were being used to carry on this racket and blocked withdrawal of the assets that were gained from the criminal proceedings.

Social Engineering Scams: We have witnessed a growth in LEA requests pertaining to social engineering scams. Social engineering attacks are usually conducted through emails, phone calls, and even text messages. Under various pretexts ranging from credit card expiry to bank account validation, the scammer tends to flag off a sense of urgency and fear with the aim to push victims to take action without careful assessment.

A few months ago, a group of criminals from Ghaziabad, Uttar Pradesh, created an elaborate fake trading app to lure customers and dupe them of huge sums of money. WazirX assisted the Ghaziabad Police real-time in identifying the identities that were linked to the culprits, which led to their arrest

Fraudulent Transactions: With the changing nature and technological advancements in business and trade, users' personal identification becomes extremely crucial in delivering services. In the case of ID theft, a scammer wrongfully obtains and uses another person's personal data with the intention of fraud or deception, typically for economic gains.

In Bandra, Mumbai, Maharashtra, the WazirX team helped identify wallets linked to Chinese loan apps that were used to dupe people through fraudulent transactions. The team worked closely with the law enforcement agency to identify the accused and block their operations.

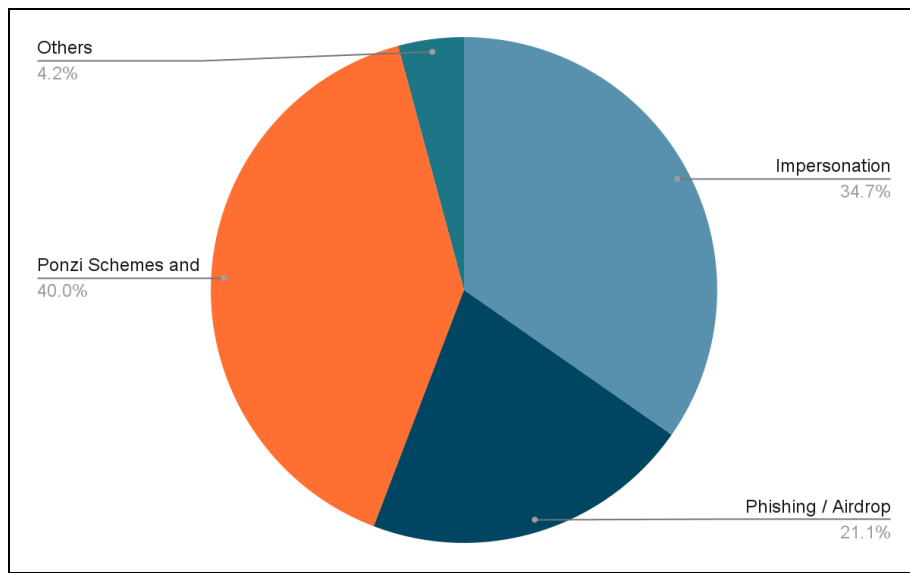
The Enforcement Directorate (ED) had conducted investigations of 16 fintech companies and Instant loan apps. Some of the suspected transactions happened on the WazirX platform. WazirX cooperated with the investigators by providing them with all the necessary details, information, and documents of the alleged accused companies who used the WazirX platform. After an in-depth internal investigation, WazirX noticed that most of the users whose information was sought by ED were already identified as suspicious by WazirX internally and were blocked in 2020-2021. Due to the active cooperation extended by WazirX and active Anti-money laundering (AML) checks, suspected users were identified.

In another incident, the legal team assisted the Kolkata police in nabbing some criminals who were defrauding people through a mobile gaming platform. In this case, a large sum of money was collected from the public via the platform called e-nuggets. The culprits then disabled withdrawal of money and also removed all data from the app. WazirX helped ED freeze crypto assets worth Rs 12.83 Crores.

In one of the first Disproportionate asset cases involving Crypto, WazirX helped Bhubaneswar Police identify the Crypto accounts of an engineer who did not reveal his investments in Digital Assets. Upon scrutiny by the team it was discovered that he had 50 odd Crypto wallets and an investment worth Rs. 2 crore.

Here is a split up of scams that were reported:

Sr.No	Categories	Percentage Share
1.	Impersonation	34.7%
2.	Phishing / Airdrop Scams	21.1%
3.	Ponzi Schemes and Social Engineering Scams	40%
4.	Others	4.2%



This chart clearly shows that the majority of scams originate from outside the on-chain crypto ecosystem.

According to our data, only 4-5% of cases are related to actual blockchain and VDA frauds, which we are assured to address with increased monitoring capabilities. Also, a clear regulatory framework could help with finer detection and resolution.

Region-wise behavior

Based on the requests received, we also mapped a state/region-wise criminal behavior that some registered users had been allegedly engaged:

- The most number of requests came in from regulators and law enforcement agencies in Maharashtra. The charges were criminal in nature, with most of them being fraudulent transactions, scams, cheating, loan app frauds, etc.
- Illegal fund transfer, Crypto scams, cheating, and forgery were the most common types of crimes reported.
- West Bengal/Eastern Region recorded a large number of cases related to identity theft, money laundering, fund misappropriation, etc.

- Foreign LEA requests were related to identifying wallets that have been accused of identity theft and scam, freezing of assets, temporary asset withdrawal suspension, monitoring assets flow, etc.

Proactive Collaboration

In order to boost better engagement and collaboration with LEAs, WazirX has initiated a mechanism for proactive reporting of suspicious transactions to law enforcement. The team shares details of accounts with suspicious transactions and also when assets are misaligned with individual ITR with the appropriate LEA. This reporting is done for both accounts deemed to be high-risk ones as well as regular users not abiding by protocol.

The team receives an alert from third party tools on every suspicious transaction, after which the account is blocked, and investigations related to fund sources, transfers, bank documents, and ID checks are carried out. Users are notified in case additional documentation is required to unblock the account. Up to 3 reminders are given before the account is blocked for a longer period.

The team then shares these details with the LEAs. The team has so far, as a matter of abundant precaution, reported over 200 transactions pertaining to 120 odd clients to the Financial Intelligence Unit of India in the months of August and September, 2022.



Building on our Transaction Monitoring Foundation

Consistent quality and risk monitoring policies

Along with robust KYC and AML policies, our collaboration with third-party forensic tool providers such as TRM Labs and Chainalysis has augmented our compliance and monitoring capabilities enabling us to track transactions continuously and investigate any suspicious activities.

- **Continuous Transaction Monitoring:** For this, every transaction's hash is passed to TRM's API, and aspects of the transaction, including the sender and recipient addresses, are screened for risk indicators. In the case of risk detection, an alert is triggered and logged into a portal. It is then reviewed and assigned to an investigator if necessary.

- **Investigations into Suspicious Activities:** If screening and monitoring systems trigger a manual review, compliance investigators use forensic tools to investigate in a more detailed manner. The transaction history and off-chain affiliations of interest are looked into.

WazirX Monitoring Approach

Strategically embedding the use of data through digital monitoring capabilities

WazirX leverages TRM labs transaction monitoring system and the data generated from it to aid in reporting to regulatory authorities and assist law enforcement agencies. Because of this, WazirX has successfully established a strong monitoring system and also simultaneously derived the below-listed benefits:

- Payments fraud intelligence
- Audit trail maintenance
- Improved TAT for compliance personnel
- Improved data quality and architecture
- Knowledge sharing capabilities.

Policy Outreach

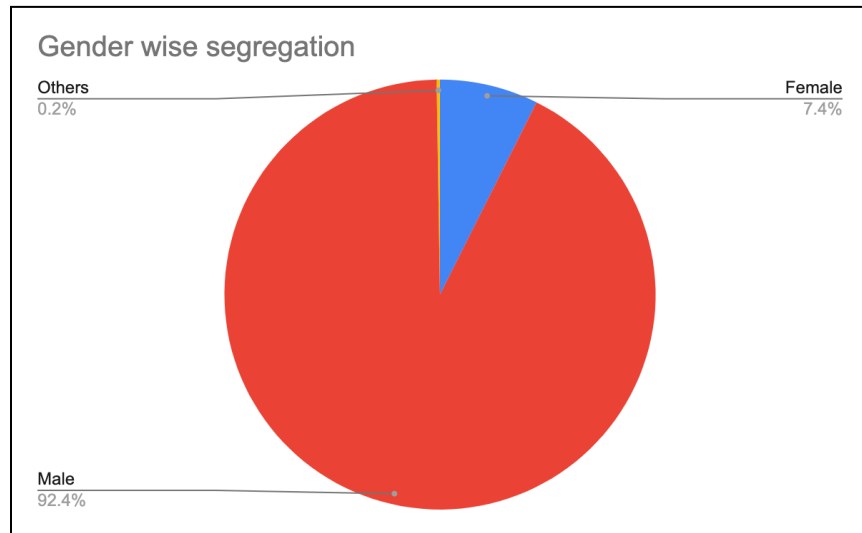
WazirX has continued its self-regulatory mechanism to promote VDAs in a responsible way. The mandated self-regulation also had industry-wide consent for educating existing users and augmenting awareness about VDA trading for prospective users to have their own strong understanding.

Collaborations

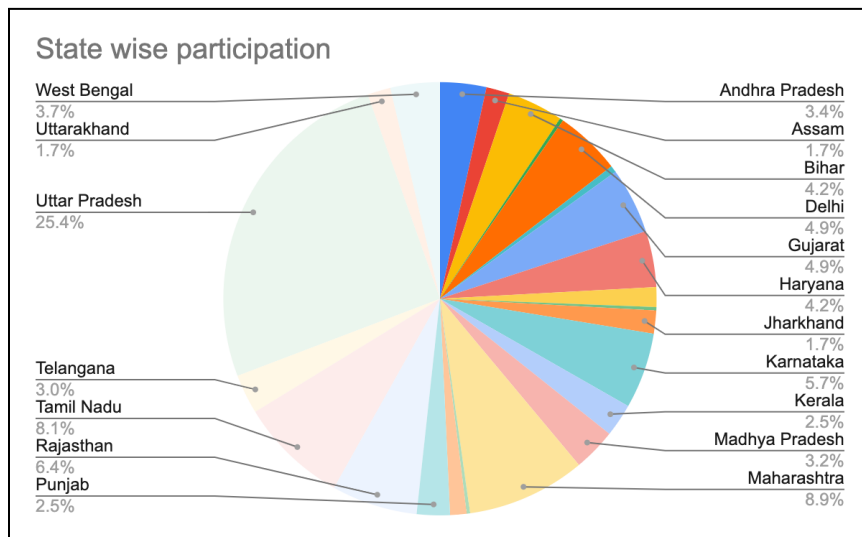
Education Program backed by UGC

With an aim to propagate the positives of Blockchain Technology and equip young individuals with in-depth knowledge about blockchain for future jobs, a free bilingual course was launched. WazirX did this in collaboration with Gurukula Kangri in Haridwar, a deemed-to-be university, as per the University Grants Commission (UGC). Since its

initiation, the course has seen more than 20,000 enrolments. We recently awarded the completion certificate to 400+ individuals. 7.4% of these were females.



Uttar Pradesh saw the highest number of enrolments in the program among all participating states.



Collaboration with law enforcement

WazirX is committed to its duties. The team has actively collaborated with several law enforcement agencies to support them, as we live in an ever-evolving tech, VDA, and Blockchain space. WazirX has designed a training module for pan-India's law enforcement community. The training includes:

- A brief history of money and crypto
- Why Blockchain matters in today's cyber economy
- How does tokenomics work, and how to value a coin?
- Application of Blockchain in Cyber Security
- Use cases of Blockchain
- Live Demo of On-chain Transaction via TRM Labs & Blockchain Explorers.

Till now, WazirX has collaborated with cybercrime establishments of more than 5 States as well as various central financial monitoring agencies.

Position Papers and Advocacy Programs

WazirX believes that the best way to increase adoption of digital assets is by raising awareness among stakeholders. WazirX conducted a day-long training program for Bhopal Cyber Crime Cell to apprise the police with knowledge and skills to identify, track and tackle any Crypto related scam.

WazirX shares reading material on its **blog** frequently and also indulges in discussions on **Discord, Twitter, Telegram, YouTube**, and more platforms.

Tackling misinformation and busting misconceptions around VDA is just one of the ways in which we can help our users make informed VDA investment decisions. As pioneers in this space, we are committed to spreading the right information to our users. We are constantly making efforts to foster a conducive environment to help the crypto community make informed choices.
